Amendments to the Claims:

Amendments to the claims are reflected in the following listing, which replaces any and all prior versions and listings of claims in the present application:

Claim Listing

1. (Currently Amended) A method for facilitating biometric security in a smartcard transaction system, said method comprising:

receiving a first proffered biometric sample and a second proffered biometric sample at a biometric sensor configured on a smartcard, wherein said smart card comprises a common application and a second application, said second application storing travel-related information associated with a cardholder, said second application comprising a common file structure and a partner file structure, and receiving a first proffered biometric sample and a second proffered biometric sample, wherein said first proffered biometric sample is a different type of biometric sample from said second proffered biometric sample, and wherein said first proffered biometric sample and said second proffered biometric sample are from the same user, and wherein said first proffered biometric sample is required to access said common file structure and said second proffered biometric sample is required to access said partner file structure;

generating data representing said first proffered biometric sample and a second proffered biometric;

~~using said data representing said proffered biometric sample as a variable in an encryption calculation to secure at least one of user data and transaction data;~~

verifying said first proffered biometric sample and a second proffered biometric; and

enabling write access to a field within said partner file structure upon verification of said second proffered biometric sample and upon request by a first partnering organization;

denying write access to said field upon request by a second partnering organization;

enabling write access for said first partnering organization and said second partnering organization to a field in said common file structure, upon verification of said first proffered biometric sample;

transferring common data to facilitate authorization of said transaction; and,

transferring said travel-related information, information related to said common file structure and information related to said partner file structure to facilitate said transaction.

~~facilitating authorization of a smartcard transaction.~~

2. (Currently Amended) The method of claim 1, further comprising registering said first proffered biometric sample and a second proffered biometric with an authorized sample receiver.

3. (Currently Amended) The method of claim 2, wherein said step of registering includes at least one of: contacting said authorized sample receiver, proffering said first proffered biometric sample and a second proffered biometric to said authorized sample receiver, associating said first proffered biometric sample and a second proffered biometric with user information, verifying said first proffered biometric sample and a second proffered biometric, and storing said first proffered biometric sample and a second proffered biometric upon verification.

4. (Cancelled).

5. (Currently Amended) The method of claim 1, wherein said step of receiving said first proffered biometric sample and a second proffered biometric further includes processing database information, wherein said database information is contained in at least one of said smartcard, a smartcard reader, said biometric sensor, a remote server, a merchant server and said smartcard system.

6. (Currently Amended) The method of claim 1, wherein said step of receiving said first proffered biometric sample and a second proffered biometric further includes comparing said first proffered biometric sample and a second proffered biometric with a stored biometric sample.

7. (Currently Amended) The method of claim 6, wherein said step of comparing includes comparing said first proffered biometric sample and a second proffered biometric to said stored biometric sample by using at least one of a third-party security vendor device and a local CPU.

8. (Cancelled).

9. (Currently Amended) The method of claim 1, wherein said step of verifying said first proffered biometric sample and a second proffered biometric further includes using a secondary security procedure, said secondary security procedure including sending a signal to notify that a requested transaction would violate an established rule for said smartcard.

10. (Currently Amended) The method of claim 1, wherein said step of receiving said first proffered biometric sample and a second proffered biometric at said biometric sensor includes receiving said first proffered biometric sample and a second proffered biometric at at least one of: a retinal scan sensor, an iris scan sensor, a fingerprint sensor, a hand print sensor, a hand geometry sensor, a voice print sensor, a vascular sensor, a facial sensor, an ear sensor, a signature sensor, a keystroke sensor, an olfactory sensor, an auditory emissions sensor, and a DNA sensor.

11. (Currently Amended) The method of claim 1, further comprising verifying whether said ~~a~~ ~~smartcard~~ transaction is in compliance with a preset transaction limitation associated with at least one of a: charge card account, credit card account, debit card account, savings account, private label account and loyalty point account.

12. (Cancelled)

13. (Currently Amended) The method of claim 1, further comprising verifying whether said ~~a~~ ~~smartcard~~ transaction is in compliance with a preset transaction limitation comprising at least one of a maximum transaction amount, minimum transaction amount, maximum number of transactions within a time period, maximum number of transactions, use by certain merchants, temporal limitation, geographic limitation, and use of non-monetary funds.

14. (Currently Amended) The method of claim 1, further comprising requiring ~~a~~ said second proffered biometric sample to override a preset transaction limitation.

15. (Cancelled).

16. (Currently Amended) The method of claim 1 ~~15~~ , further comprising accessing card-holder preferences relating to at least one of rental cars, hotel reservations, and air travel in said ~~first~~ partner file structure, upon verification of said second proffered biometric sample.

17. (Previously Presented) The method of claim 16, further comprising updating said card-holder preferences relating to at least one of rental cars, hotel reservations, and air travel in said first partner file structure.

18. (Cancelled)

19. (Currently Amended) The method of claim 1, further comprising using said data representing said first proffered biometric sample and a second proffered biometric as at least one of a private key, a public key, and a message authentication code to facilitate transaction security measures.

20. (Currently Amended) The method of claim 1, further comprising using said data representing said first proffered biometric sample and a second proffered biometric in generating a message authentication code and as at least one of a private key and a public key.

21. (Currently Amended) The method of claim 1, further comprising using said data representing said first proffered biometric sample and a second proffered biometric to facilitate substantially simultaneous access to goods and initiation of authentication for a subsequent purchase of said goods.

22. (Cancelled).

23. (New) The method of claim 1, further comprising writing to at least one of said partner file structure and said common file structure to program said smartcard as a room key.

24. (New) The method of claim 1, further comprising:

storing, by a first enterprise data collection unit, update transactions and pending transactions associated with said smartcard and a first enterprise, wherein said first enterprise data collection unit is associated with a first enterprise;

storing, by a second enterprise data collection unit, update transactions and pending transactions associated with said smartcard and a second enterprise, wherein said second enterprise data collection unit is associated with a second enterprise;

interfacing with said smartcard and said first and second enterprise data collection units, at an access point;

storing, by a card object database system coupled to said first and second enterprise data collection units, said smartcard information in accordance with said update transactions and said pending transactions, wherein said smartcard information includes a card object having an application;

routing, by an update logic system, said smartcard information from said first and second enterprise data collection units to said access point in order to effect synchronization of said smartcard information associated with said smartcard and said card object database system; and,

activating, by said verification device, said update logic system upon verification of said first proffered biometric sample and said second proffered biometric sample.

25. (New) The method of claim 24, further comprising securely routing, by an update logic system, card information between said enterprise data synchronization interface and said enterprise data collection units, wherein said update logic system is coupled to an enterprise data synchronization interface, and communicating, by said enterprise network, with said access point, wherein said enterprise data synchronization interface is coupled to said enterprise network.

26. (New) The method of claim 25, further comprising, by a secure support client server, communicating with said access point, and adaptively providing communication functionality in accordance with the communication functionality available at said access point.

27. (New) The method of claim 26, further comprising:

communicating, by a key system, with a security server and supplying a key in response to a request from said security server, wherein said key system is associated with said application;

receiving, by a personalization utility, said card object and communicating with said security server;

adding, by said personalization utility, said key to said card object;

accepting, by a card management system, a card request and communicating said card request to said personalization utility; and

communicating, by a gather application module, with said card management system and gathering application information from a first database and a second database in accordance with said card request, wherein said first database is associated with said first enterprise, and said second database is associated with said second enterprise.

28. (New) The method of claim 1, further comprising displaying a first plurality of financial accounts upon verification of said first proffered biometric sample, and displaying a second plurality of financial accounts upon verification of said second biometric sample, wherein said first plurality of financial accounts include different financial accounts than said second plurality of financial accounts.

29. (New) The method of claim 1, further comprising associating a first set of rules with said first proffered biometric sample and displaying a first plurality of financial accounts upon verification of said first proffered biometric sample and said first set of rules, and associating a second set of rules with said second proffered biometric sample and displaying a second plurality of financial accounts upon verification of said second biometric sample and said second set of rules, wherein said first plurality of financial accounts include different financial accounts than said second plurality of financial accounts.